7. Wireshark Basics

🕵️ Wireshark

1. What is Wireshark?

- Wireshark is a **free and open-source** network protocol analyzer used for **network troubleshooting, analysis, and cybersecurity investigations**.
- It captures live network traffic (packets) in real-time and allows detailed inspection of hundreds of protocols at multiple layers of the OSI model.
- Essential for **packet-level forensic analysis**, identifying network anomalies, debugging protocols, and reverse-engineering attacks.
- Supports live capture or analysis of saved capture files (`.pcap`, `.pcapng`).

2. How to Use Wireshark Filters

Wireshark uses **two main types of filters** to help focus on relevant packets:

a. Capture Filters

- Applied **before** packet capture starts.
- Limit what packets get saved for analysis (reduces noise).
- Use **Berkeley Packet Filter (BPF)** syntax (similar to tcpdump).
- Example:
  - Capture only TCP traffic on port 80:

    ```
    tcp port 80
    ```

  - Capture traffic from a specific IP:

    ```
    host 192.168.1.10
    ```

- Set in the capture options before starting capture.

b. Display Filters

- Applied **after** capture, to filter displayed packets without discarding data.
- Use Wireshark's own syntax, more powerful and flexible.
- Examples:
  - Show only HTTP packets:

    ```
    http
    ```

- Show traffic to or from a particular IP:

  ```
  ip.addr == 192.168.1.10
  ```

- Show TCP packets with SYN flag set (connection initiations):

  ```
  tcp.flags.syn == 1 && tcp.flags.ack == 0
  ```

- You type these filters in the filter toolbar and press Enter.

---

3. Analyzing a Packet with Wireshark

Step-by-step process:

1. **Open Wireshark & capture or load a pcap file.**
2. **Select a packet from the packet list pane (top section).**
3. **Inspect packet details pane (middle section):**
   - Displays decoded protocol layers from **frame level** to **application protocols**.
   - Expand each layer to see detailed fields and flags (e.g., Ethernet header, IP header, TCP header, HTTP payload).
4. **Follow streams:**
   - For protocols like TCP, right-click a packet and choose **"Follow TCP Stream"** to reconstruct full conversations for easier analysis.
5. **Use color coding:**
   - Wireshark colors packets by protocol or anomaly type to visually identify interesting packets quickly.
6. **Check packet bytes pane (bottom section):**
   - Shows raw hexadecimal and ASCII representation of the packet payload.
   - Useful for manual inspection of data, hidden payloads, or exploits.
7. **Use filters to narrow down suspicious traffic** based on IPs, protocols, ports, flags, payload content, or error flags.
8. **Export packets or conversations** for further offline analysis or reporting.

Summary: Wireshark is a **powerful tool** for deep packet-level insight into network traffic, essential for identifying threats, debugging protocols, and incident investigation. Mastering capture and display filters is critical for efficient analysis.
